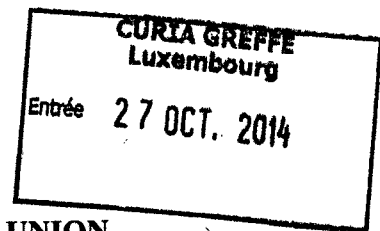




Date de réception : 23/01/2015



COURT OF JUSTICE OF THE EUROPEAN UNION

Preliminary Reference in Case C-362/14

Between:-

MAXIMILLIAN SCHREMS

Applicant

-and-

DATA PROTECTION COMMISSIONER

Respondent

OUTLINE WRITTEN SUBMISSIONS OF THE
DATA PROTECTION COMMISSIONER

CONTENTS

- A) Introduction.
- B) The nature of the opinion formed by the DP Commissioner.
- C) The relevant legal framework.
- D) The position of the DP Commissioner in this case.
- E) Conclusion.

Registered at the Court of Justice under No.	976670
Luxembourg,	27. 10. 2014 For the Registrar
Fax/E-mail:	24.10.14 [Redacted]
Received on:	27.10.14 Lynn Hewlett Principal Administrator

A) INTRODUCTION

Background to the judicial review that led to this request for a preliminary ruling

- 1) Facebook Ireland Limited is a limited liability having its registered office at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.
- 2) All subscribers to the *Facebook* social media platform who are resident in the European Union / European Economic Area are required to enter into contract with Facebook Ireland Limited.
- 3) On 25 June 2013¹, the Applicant made a complaint to the Data Protection Commissioner (“**the DP Commissioner**”) alleging that:
 - (i) Facebook Ireland Limited was transferring personal data relating to Facebook subscribers resident in the EU/EEA to servers located in the United States, owned or controlled by its parent company, Facebook Inc.; and,
 - (ii) Facebook Inc. was in turn providing the United States National Security Agency with direct and unhindered access to bulk data held on its servers, including data relating to Facebook subscribers resident in the EU/EEA.
- 4) The Applicant’s complaint was based on the revelations made by Edward Snowden to the effect that the National Security Agency had established a programme (referred to as the “PRISM” programme) under which it obtained unhindered access to bulk data held on servers located in the United States, owned and/or controlled, not just by the operators of the *Facebook* social media platform, but by a range of different internet and technology companies, including Apple, Skype, Microsoft, and others.
- 5) The DP Commissioner formed the opinion that the Applicant’s complaint should not be admitted to investigation as the complaint was bound to fail. As such, it was properly to be considered “frivolous or vexatious” within the narrow, technical meaning of those

¹ See Attachment 1

words as used in Section 10(1)(b)(i) of the DP Acts. The DP Commissioner formed that opinion in light of the following:

- (i) Section 11 of the Data Protection Acts 1988-2003² (“**the DP Acts**”);
 - (ii) Commission Decision No. C2000/520/EC³ (“**the Commission Decision**”);
 - (iii) the terms of the Safe Harbour Privacy Principles and FAQs; and,
 - (iv) Facebook’s self-certified adherence to the Safe Harbour Principles and FAQs⁴ (such certification having been verified by the DP Commissioner’s office by examining entries noted on a publicly-accessible register operated by the United States Department of Commerce).
- 6) In the judicial review that has led to this request for a preliminary ruling the Applicant seeks to quash the opinion formed by the DP Commissioner that his complaint should not be admitted to investigation. It is to be noted that the Applicant did not bring any challenge to the validity of the 1995 Directive or the Commission Decision in his proceedings.
- 7) The desired outcome that the Applicant sought from his proceedings before the Irish courts is apparent from his letter of complaint dated 25 June 2013 in which he sought the following of the DP Commissioner:
- (i) That the DP Commissioner review the validity of the Commission Decision, which in turn incorporates the Safe Harbour Privacy Principles and FAQs;
 - (ii) If necessary, that the DP Commissioner obtain a preliminary ruling from the CJEU on the validity of the Commission Decision; and,
 - (iii) If necessary, that the DP Commissioner prohibit the transfer of personal data by Facebook Ireland Limited to Facebook Inc. unless Facebook Ireland

² See Attachment 2

³ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=EN>

⁴ <http://safeharbor.export.gov/companyinfo.aspx?id=23019>

Limited could disprove reports of the “PRISM” programme.

The nature of the question raised before this Court

- 8) The question raised before this Court is essentially a jurisdictional question, namely, whether it was open to the DP Commissioner to challenge the Safe Harbour Principles and FAQ on the grounds advanced by the Applicant, in circumstances where the DP Commissioner is bound by the terms of the Commission Decision.
- 9) The DP Commissioner submits that he acted within jurisdiction in declining to investigate the complaint in circumstances where:
 - i) The Commission Decision represents a “Community Finding” within the meaning of that term as set out in Section 11(2)(a) of the DP Acts, which in turn follows the provisions of Article 25(6) of the Directive 95/46/EC⁵ (“the 1995 Directive”);
 - ii) Under Section 11 of the DP Acts, the DP Commissioner is bound to apply that Community Finding; and,
 - iii) The Applicant did not allege that there was a substantial likelihood that the Safe Harbour Privacy Principles and FAQ are being violated by Facebook Ireland Limited and/or Facebook Inc. Nor did he provide evidence of any such violation. Accordingly, the complaint made did not engage Article 3 of the Commission Decision. On the contrary, the Applicant sought to challenge the terms of the Safe Harbour regime itself on the grounds that there is no meaningful protection in United States’ law and practice in respect of data transferred to the United States, so far as State surveillance is concerned.
- 10) In these circumstances, it is submitted that the actions of the DP Commissioner demonstrated scrupulous adherence to the application of the law as he understands it to

⁵ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&qid=1414083125498&from=EN>

be, represented by the 1995 Directive and the terms of the Commission Decision.

- 11) As regards the substantive question of whether a National Data Protection Authority can and/or should look behind a Community Finding in order to preserve the rights of individuals (and the particular circumstances in which that approach might be taken), it is submitted that any substantive discussion of these issues is properly a matter for the EU Commission and the Member States themselves.
- 12) The DP Commissioner acknowledges that this referral raises important and complex legal issues regarding how, and by whom, the rights of individuals are to be vindicated in this rapidly developing area. The DP Commissioner welcomes the clarity that will be brought to these issues by this referral.
- 13) It is emphasized that, in the proceedings before the Irish High Court, the Applicant chose not to bring any challenge to the validity of the 1995 Directive or the Commission Decision. Rather his challenge was limited to the opinion formed by the DP Commissioner that the Applicant's complaint should not be admitted to investigation for the reasons outlined (in summary terms) at paragraph 5 above.

B) NATURE OF OPINION FORMED BY THE DP COMMISSIONER

- 14) As noted above, the proceedings before the Irish High Court arose from a challenge to the fact that DP Commissioner declined to investigate the complaint having formed the opinion that it was unsustainable in law or, to use the language of Section 10(1)(b)(i) of the DP Acts, the complaint was "frivolous or vexatious".
- 15) In *Nowak v Data Protection Commissioner*⁶ the Irish High Court (Birmingham J) explained the nature of such an opinion formed under Section 10(1)(b)(i) in the following terms:

"Once the Commissioner had formed the view that the examination script did not constitute personal data it followed that he was being asked to proceed with

⁶ [2013] 1 ILRM 207; see Attachment 3.

an investigation where no breach of the Data Protection Acts could be identified. It was in those circumstances he had resort to s. 10(1)(b)(i). That section refers to complaints that are frivolous or vexatious. However, I do not understand these terms to be necessarily pejorative. Frivolous, in this context does not mean only foolish or silly, but rather a complaint that was futile, or misconceived or hopeless in the sense that it was incapable of achieving the desired outcome..." (page 216)(emphasis added).

- 16) Similarly, in the judgment delivered in these proceedings in the Irish High Court, Hogan J made the following observations (at paragraph 39 of his judgment⁷) on the meaning of the words "frivolous and vexatious" as used in the particular context of Section 10(1)(b)(i) of the DP Acts:

"It is certainly true that in the ordinary sense of these words the present complaint – raising as it does weighty issues of transcendent importance in relation to data protection – is neither "frivolous" nor "vexatious". While in this respect the actual language of s.10(1)(b) of the 1988 Act is somewhat unfortunate and perhaps even unhelpful, nevertheless, as Birmingham J. pointed out in Novak, in this particular statutory context these words also apply to a case where the claim is considered to be unsustainable in law."

- 17) It is also relevant to note that the forming of an opinion by the DP Commissioner at a particular point in time that a particular complaint is not admissible is not necessarily a final one for all time. Nor does it preclude a fresh complaint being made if the law changes or if further evidence becomes available. For example, if the Commission Decision were to be revoked and/or replaced at some future date then clearly any new complaint that the Applicant might wish to bring would fall to be considered under the new legal regime in place. However the DP Commissioner has to have regard to the state of the law as it stands at the time when he is considering a particular complaint. That is what was done in this case.

⁷ [2014] IEHC 310; see Attachment 4.

C) THE RELEVANT LEGAL FRAMEWORK

Domestic law

- 18) Ireland has implemented its obligations as regards data protection into domestic law by means of the DP Acts. The DP Commissioner is established pursuant to those Acts and is bound by them in terms of the scope of his powers.
- 19) Section 10(1) of the DP Acts provides for the power to investigate complaints and states that:
- (a) The DP Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.
 - (b) Where a complaint is made to the DP Commissioner under paragraph (a) of this subsection, the DP Commissioner shall-
 - (i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and,
 - (ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.

In this case the DP Commissioner formed the opinion that the Applicant's complaint was "frivolous or vexatious" in the sense that it was bound to fail for the reasons summarized at paragraph 5 above. On that basis, he declined to investigate the

complaint.

- 20) Section 11 of the DP Acts addresses the issue of the transfer of personal data outside of the State. Section 11(2)(a), which was inserted by the Data Protection (Amendment) Act, 2003, provides that the DP Commissioner is bound by a Community Finding:

- (a) Where in any proceedings under this Act a question arises-
 - (i) whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred, and
 - (ii) a Community finding has been made in relation to transfers of the kind in question,

the question shall be determined in accordance with that finding.

- 21) Section 11(2)(b) of the DP Acts defines the concept of a Community finding in the following terms:

“In paragraph (a) of this subsection ‘Community finding’ means a finding of the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of the Directive under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area.”

- 22) The Commission Decision is made pursuant to Article 25(6) of the 1995 Directive and so comes within the definition of a ‘Community finding’.
- 23) Section 11(2) of the DP Acts makes it clear that where matters relating to international data transfer out of the EU have been dealt with at an EU level then it is not for domestic regulators to seek to go behind that. One can readily see the logic of this since

it would be very difficult for the EU to trade with the United States if every Member State took a different approach to this issue. It is the type of issue that is more appropriately dealt with at an inter-governmental level with the involvement of bodies such as the Commission and the Parliament.

- 24) There are also practical difficulties which arise out of a domestic regulator seeking to engage with political, diplomatic and trade issues. It is also difficult to see how a single domestic regulator can police what does or does not happen in the United States. The DP Commissioner's powers under the DP Acts are not extra-territorial.

EU law

- 25) The DP Acts were enacted to give effect to the Data Protection Convention 1981⁸ and the 1995 Directive.
- 26) Article 16 of the Treaty on the Functioning of the European Union⁹ also makes express reference to the need to protect personal data and provides that "Everyone has the right to protection of personal data concerning him or her." Article 8(1) of the Charter of Fundamental Rights of the European Union¹⁰ is expressed in precisely the same terms. The Charter goes on to provide as follows at Articles 8(2) and 8(3):

"2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which had been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

⁸ <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

⁹ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=en>

¹⁰ http://www.europarl.europa.eu/charter/pdf/text_en.pdf

- 27) In respect of some countries (such as Argentina, Canada, Israel and Switzerland) the Commission has issued individual decisions recognising them as providing adequate protection for personal data on the basis that those countries have generally applicable data protection laws which follow the approach of the Directive.
- 28) The Commission Decision was adopted to establish the Safe Harbour Principles and FAQs as a reference point for permissible data transfers to the United States on the basis that the United States has a different approach to data protection than the EU (being based on piece-meal legislation, self-regulation and consumer action). The Safe Harbour regime was introduced against the backdrop of concerns that personal data would stop flowing to the United States after the implementation of the 1995 Directive in the EU.¹¹ The Safe Harbour Privacy Principles and FAQs were issued by the United States Department of Commerce on 21 July 2000 and, following the adoption of the Commission Decision on 26 July 2000, they came into effect in November 2000.
- 29) The Commission Decision is thus the relevant 'Community finding' that governs this area of the law and, as such, the DP Commissioner is bound to take notice of it and to apply it.
- 30) Participation by individual organisations in the Safe Harbour framework is voluntary. Where an organisation elects to participate, however, it is required to certify to the United States Department of Commerce that it is operating in compliance with the Safe Harbour Privacy Principles and FAQs. Amongst other things, it must adopt a publicly stated privacy policy incorporating the standards set out in the Privacy Principles and the FAQs. Upon so certifying, the Privacy Principles and FAQs become legally binding on the organisation in question and they may be enforced against it. Certification remains in force for a period of 12 months following which it may be renewed. The organisation must make an annual return to the Department of Commerce confirming its continued compliance.

¹¹ See generally Jay, *Data Protection Law and Practice* (Sweet and Maxwell, 4th ed. 2012), Chapter 8; see Attachment 5.

- 31) Participants in the framework are required to adopt effective and independent complaints and dispute resolution procedures. Separately, and depending on the particular sector in which they operate, they must subject themselves to regulation by the Federal Trade Commission or the United States' Department of Transportation.
- 32) The United States' Department of Commerce maintains a publicly accessible list¹² of participants in the Safe Harbour scheme. Amongst other things, the listing identifies the enforcement and independent dispute resolution agency applicable to each participant.
- 33) Failure to comply with the Safe Harbour Privacy Principles and FAQs in the United States can result in an organisation being the subject of enforcement proceedings by the Federal Trade Commission. In the context of such proceedings, the Commission may impose significant financial penalties. It may also direct the strike-off of an organisation from the above-referred list, causing the organisation to lose its Safe Harbour status.
- 34) Recital 9 of the Commission Decision expressly recognises that it may need to be reviewed by the EU in the light of experience:

“The ‘safe harbor’ created by the Principles and the FAQs, may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved.”

The DP Commissioner notes that a detailed review of the operation and effectiveness of the Safe Harbour scheme is presently underway and that changes to the scheme are the subject of ongoing negotiations between the Commission and the United States.

- 35) Article 4 of the Commission Decision provides:

“This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the

¹² <http://safeharbor.export.gov/list.aspx>

Principles and the FAQs is overtaken by the requirements of US legislation.”

36) Obviously the form of review and/or adaptations contemplated by Article 4 will occur at an EU and/or EU-US level. The DP Commissioner does not believe that it is his role to pre-empt what the outcome of the current review may be.

37) The Safe Harbour Principles set out at Annex 1 of the Commission Decision expressly state that:

“adherence to these principles may be limited (a) to the extent necessary to meet national security, public interest or law enforcement requirements” .

38) The preamble to the Principles:

“US law will apply to questions of interpretation and compliance with the Safe Harbour Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbour organisations, except where organisations have committed to cooperate with European Data Protection Authorities ...” .

39) Under Article 3 of the Commission Decision, a national Data Protection Authority can direct the suspension of data flows to an entity that has self-certified its adherence to the safe harbour principles in two specific scenarios:

(i) Where a relevant US enforcement authority has determined that the receiving entity is violating the safe harbour principles; or,

(ii) Where the following circumstances arise:

(a) There is a substantial likelihood that the Principles are being violated;

(b) There is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue;

(c) The continuing transfer would create an imminent risk of grave harm to data subjects; and,

(d) The competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

40) It is clear that (i) has no application to this case. So far as (ii) is concerned, the position is as follows.

41) In this case, no evidence was put before the DP Commissioner by the Applicant on which the DP Commissioner could have concluded that there was a *substantial* likelihood that the Safe Harbour Principles were in fact being violated specifically in the case of the data transfers referenced by the Applicant, i.e. data transfers between Facebook Ireland Limited and Facebook Inc. On the contrary, the Applicant's complaint was presented in generalised and essentially speculative terms. It is also of note that the Applicant did not adduce evidence to suggest that there was an imminent risk of grave harm to him, or that any of *his* data had been or was likely to be accessed by the National Security Agency. Rather, the complaint appeared to be made in a representative capacity on behalf of Facebook subscribers' generally.

42) Equally, the Applicant put forward no factual or other material on which the DP Commissioner could reasonably have concluded that the enforcement mechanisms provided for under the Safe Harbour Privacy Principles were not addressing (and would not address) the issues raised insofar as they affected the Applicant, or that the relevant enforcement and/or dispute resolution agency would not "take adequate and timely steps to settle the case at issue". Indeed, it is clear that, as at the date of submission of his complaint to the DP Commissioner, the Applicant had not sought to have recourse to the enforcement mechanisms provided for under the Safe Harbour Privacy Principles.¹³

¹³ It appears that the Applicant may have sought to engage the Safe Harbour dispute resolution mechanism after the DP Commissioner had declined to investigate his complaint, and after the Applicant had already commenced judicial review proceedings against the DP Commissioner in the Irish High Court. At the hearing of the judicial

- 43) Nor is it clear how the DP Commissioner could himself have investigated or determined whether, for example, the NSA was accessing Facebook subscriber data at all, or in a way, or to an extent, that was not consistent with the Safe Harbour Privacy Principles and/or national or European data protection law. As noted at paragraphs 15, 23 and 25 of his First Affidavit, the DP Commissioner did in fact obtain confirmation from Facebook Ireland Limited (being the transferring party referenced by the Applicant) that the media reports on which the Applicant's complaint rested (being reports to the effect that the NSA was in a position to obtain direct and unhindered access to bulk data held on servers located in the United States relating to Facebook subscribers) were not correct.
- 44) Against this backdrop, and in circumstances where the EU Commission was already engaged in a substantial review of the operation of the Safe Harbour scheme with a view to effecting material changes to that scheme, the DP Commissioner took the view that the Applicant's complaint should properly be addressed at EU level and not by a national data protection commissioner.

The scope of the DP Commissioner's role in domestic law

- 45) It may be of assistance to the Court to make some observations on the legal nature of the DP Commissioner under Irish law. The DP Commissioner has jurisdiction to make decisions in respect of complaints that have first been admitted to investigation. Where a party to whom a decision is directed is dissatisfied, they may avail of a statutory appeal mechanism under which the decision will be the subject of a review by the Circuit Court. The DP Commissioner cannot award damages to a complainant. The fact that a complaint has been made to the DP Commissioner does not preclude a member of the public from litigating a grievance against someone who he believes has misused his data. By way of example Section 7 of the DP Acts provides that:

review proceedings on 30 April 2014, the Applicant produced, for the first time, a copy email dated 2 December 2013, received by him from TRUSTe, the dispute resolution entity named in Facebook Inc.'s Safe Harbour certificate. A request made by the Applicant to admit that email in evidence was denied by the Court on the basis that it post-dated the DP Commissioner's consideration of the Applicant's complaint. The Applicant's email, to which TRUSTe was replying, has not been available by the Applicant. (A copy of the email of 2 December 2013 is included as Attachment 6).

“For the purposes of the law of torts and to the extent that that law does not so provide, a person, being a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned...”

D) THE POSITION OF THE DP COMMISSIONER IN THIS CASE

- 46) The DP Commissioner formed the opinion that the Applicant’s complaint should not be admitted to investigation on the basis that the complaint was not sustainable in law in light of:
- (i) Section 11 of the DP Acts;
 - (ii) The Commission Decision;
 - (iii) the terms of the Safe Harbour Privacy Principles and FAQs; and,
 - (iv) Facebook’s self-certified adherence to the Safe Harbour Principles and FAQs.
- 47) Put simply, the DP Commissioner considered that, in the particular circumstances that obtained, he was statutorily bound to accept that a transfer of subscriber data by Facebook Ireland Limited to Facebook Inc., undertaken under and in accordance with the Safe Harbour Privacy Principles and FAQs, is lawful, and remains lawful even where such data is accessed by national security authorities in the United States having regard to the express provision made in the Safe Harbour Privacy Principles and FAQs for third party access to the extent necessary to meet national security requirements.
- 48) Data protection is a rapidly developing area of the law and, in particular, there is an on-going and intensive debate taking place at an institutional level within the EU in relation to the capacity of the Safe Harbour Privacy Principles to provide adequate protection for the data privacy rights of citizens of the European Union whose personal data is transferred to the United States. The manner in which the EU interacts with the

United States in this context is clearly a matter that falls to be determined in the first instance by way of negotiations between the EU and the United States. Against that backdrop, and in the context of the development of specific legislative proposals for revisions to the existing Safe Harbour regime, a Communication¹⁴ was issued by the European Commission on 27 November 2013, directed to the European Parliament and Council, in which the Commission recommended thirteen separate adjustments to the Safe Harbour Privacy Principles to address concerns raised about the operation of the Safe Harbour scheme in terms of transparency, availability of redress, enforcement, and access by United States authorities to transferred data. These recommendations remain the subject of discussion at EU level. They are also the subject of direct engagement between the EU and the United States in the context of ongoing dialogue between their respective justice and home affairs ministerial representatives.

- 49) So far as the subject matter of the Applicant's complaint is concerned, the Communication of 27 November 2013 contained recommendations under the heading "Access by US authorities", expressed in the following terms:

"12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate."

- 50) On the same date, a report¹⁵ was published by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection. Amongst other things, the report presents certain

¹⁴ http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

¹⁵ <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>

findings made by the EU co-chairs in connection with the legal basis on which surveillance programmes are in fact carried out by United States security agencies and the oversight and redress mechanisms to which they are subject.

- 51) For its part, the European Parliament has considered a report¹⁶ dated 8 January 2014, prepared by the Parliament's Committee on Civil Liberties, Justice and Home Affairs on "the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." On the basis of its consideration of that report, the Parliament adopted a resolution¹⁷ on 12 March 2014 in which (amongst other things) it called on the United States authorities to put forward a proposal for a new framework for transfers of personal data from the EU to the United States, to be substituted for the Safe Harbour framework, and which would meet EU law data protection requirements.
- 52) The DP Commissioner understands that, as of the date of delivery of these submissions, negotiations between the EU Commission and the United States in relation to changes demanded by the EU Commission to the Safe Harbour scheme remain ongoing.
- 53) From the outset of dealing with the Applicant's complaint the DP Commissioner emphasised the importance of the fact that the issues surrounding the 'PRISM' programme are the subject of active and ongoing engagement at an EU level and at inter-governmental level. Thus in the DP Commissioner's letter of reply dated 23 July 2013 he stated:

*"We are aware of and welcome the fact that proportionality and oversight arrangements for programmes such as PRISM are to be the subject of high-level discussions between the EU and the USA."*¹⁸

¹⁶ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN>

¹⁷ <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230>

¹⁸ See Attachment 7.

54) The DP Commissioner also noted the fact that the Applicant neither alleged, nor provided evidence, that any of his own personal data had been disclosed to US security authorities. Thus in the DP Commissioner's letter of reply dated 25 July 2013 he stated:

*"In making this assessment, the DP Commissioner is mindful of the fact that there is no evidence – and you have not asserted – that your personal data has been disclosed to the US authorities."*¹⁹

55) By way of further illustration of the nature and extent of the on-going debate in this area, the documents that were adverted to in the affidavits and in the submissions of the Applicant before the Irish High Court include the following:

- (i) Working Party Document on transfers of data to third countries²⁰ (24 July 1998);
- (ii) Working Party Document on SWIFT²¹ (22 November 2006);
- (iii) Letter from Article 29 Data Protection Working Party to Vice President of the European Commission Viviane Reding²² (13 August 2013);
- (iv) Speech of European Data Protection Supervisor to EU Parliament²³ (7 October 2013);
- (v) Communication from the European Commission to the Parliament and the Council²⁴ (27 November 2013);
- (vi) Report on the Findings by the EU Co-Chairs of the ad hoc EU-US Working Group on Data Protection²⁵ (27 November 2013);

¹⁹ See Attachment 8.

²⁰ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

²¹ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf

²² http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf

²³ https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

²⁴ http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

- (vii) Draft Report of European Parliament Committee on Civil Liberties, Justice and Home Affairs²⁶ (8 January 2014) (subsequently adopted as a resolution of the European Parliament on 12 March 2014);
- (viii) Article 29 Data Protection Working Party Document on surveillance of electronic communications for intelligence and national security purposes²⁷ (10 April 2014);
- (ix) Letter from Article 29 Data Working Party to Vice President of the European Commission Viviane Reding²⁸ (10 April 2014);

Even this list does not capture the full extent of the exchanges that have taken place (and the reports delivered) in relation to the operation of the Safe Harbour framework.

- 56) Given these ongoing and substantial developments at EU and inter-governmental level (to which the DP Commissioner is party in his capacity as a member of the Article 29 Working Group on Data Protection), we are a long way from the decision of the English courts in *N.S. v Secretary of State for the Home Department*²⁹ where Member States were seeking to return asylum seekers to Greece even though they were fully aware that the Greek system had practically ground to a halt due to the fact that almost 90% of all illegal immigrants entering the EU in 2010 came into Greece (see para 87 of the decision). As set out above, in the present case, the DP Commissioner expressly noted the fact that proportionality and oversight arrangements for security programmes impacting on the data privacy rights of citizens are the subject of ongoing high-level discussions between the EU and the United States.

²⁵ <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>

²⁶ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN>

²⁷ http://www.cnpd.public.lu/fr/publications/groupe-art29/wp215_en.pdf

²⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

²⁹ [2013] QB 102; see Attachment 9.

- 57) Finally it may be noted that the recent decision of the CJEU in *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources*³⁰ was a case where the High Court in Ireland had been asked in plenary proceedings brought against the State to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005. The High Court in Ireland had made a reference to the ECJ to determine the validity of the Directive. Clearly it cannot be suggested that the DP Commissioner in this case had jurisdiction to declare any Irish or EU law to be invalid. The CJEU concluded that the Directive was invalid and stated:

“... the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data ...” (para 54)

This is obviously a ruling that the Member States will have to pay regard to if they decide to amend the Commission Decision and to adjust the Safe Harbour Privacy Principles and FAQs previously agreed with the United States.

E) CONCLUSION

- 58) In conclusion, for all of the above reasons, it is submitted by the DP Commissioner that the answer to the first question posed by the Irish High Court is “Yes” and the answer to the second question (posed in the alternative) is “No”.

Paul Anthony McDermott

³⁰ [2014] EUECJ C-293/12, (unreported, Grand Chamber, 8th April 2014); see Attachment 10.

APPENDIX

(Documents included as attachments to these submissions)

1. Letter from Maximillian Schrems to the Data Protection Commissioner, 25 June 2013
2. Data Protection Acts, 1988 & 2003 (consolidated version)
3. *Nowak v Data Protection Commissioner* [2013] 1 ILRM 207
4. *Maximillian Schrems v Data Protection Commissioner* [2014] IEHC 310
5. Jay, *Data Protection Law and Practice* (Sweet and Maxwell, 4th ed. 2012), Chapter 8
6. Email response from the Safe Harbour/TRUSTe Feedback and Resolution System, 2 December 2013
7. Letter from the Data Protection Commissioner to Maximillian Schrems, 23 July 2013
8. Letter from the Data Protection Commissioner to Maximillian Schrems, 25 July 2013
9. *N.S. v Secretary of State for the Home Department* [2013] QB 102
10. *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* [2014] EUECJ C-293/12, (unreported, Grand Chamber, 8th April 2014)

Signed: 

Damien Young
Philip Lee
Solicitors for the Data Protection Commissioner
7 – 8 Wilton Terrace
Dublin 2
IRELAND

24 October 2014